REMARKS

In the Office Action mailed May 11, 2007 (hereinafter "Office Action"), Claims 1, 3, 5-7, 9, 10, 12-19, 24-26, 30-37, 41-45, and 47-49 were rejected under 35 U.S.C. § 103(a) as being obvious over U.S. Patent No. 6,260,145, issued to Komura et al. (hereinafter "Komura et al.") in view of U.S. Patent Application Publication No. 2002/0062440, to Akama (hereinafter "Akama"). Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 were rejected under 35 U.S.C. § 103(a) as unpatentable over Komura et al. in view Akama further in view of U.S. Patent No. 6,715,073, issued to An et al. (hereinafter "An et al.").

For the following reasons, applicant submits that the claims of the present application are not anticipated or obvious over the cited and applied prior art, alone or in combination, because the prior art fails to teach or suggest a document processing server which encrypts and processes the document obtained from a sender such that the electronic document is first encrypted with an encryption key corresponding solely to the sender and the document processing server. Additionally, the prior art fails to teach or suggestion that the document processing server provides the processed document to recipients while encrypting the electronic document with an encryption key corresponding solely to at least one recipient and the document processing server. Prior to discussing more detailed reasons why applicant believes that the claims of the present application are allowable, a brief description of the present invention and the cited references are presented.

Summary of the Claimed Invention

In accordance with the present invention, a system and method for processing communications between a sender computing device and at least one recipient computing device utilizing a document processing server are provided. The document process server is a separate entity from the sender computing device and recipient computing devices. Initially, a sender establishes a secure communication with the *document processing server* and requests the processing of an electronic document, which can include the appending of a digital signature.

The document processing server processes the electronic document and establishes secure communications with one or more designated recipients. Further, upon the sender's request, the document processing server implements sender-specified recipient identity verification and provides further processing of the electronic document as designated by the recipients. In this manner, the sender and the designated recipient do not have to generate, store or exchange any shared encryption keys, including a private encryption key, since the sender and the recipient communicate only with the document processing server, not each other. Thus, the document processing server processes the electronic document obtained from the sender with an encryption key corresponding solely to the sender and generated and stored by the document processing server on behalf of the sender. Additionally, to send the electronic document to the verified recipient, the document processing server encrypts the electronic document with an encryption key corresponding solely to the verified recipient and generated and stored by the document processing server on behalf of the verified recipient. The document processing server is responsible for any processing relating to identification and encryption/decryption of the document.

Summary of Komura et al. (U.S. Patent No. 6,260,145)

Komura et al. discloses a system and method for authenticating digital information. Initially, a server appends verification data to an electronic document to be circulated through terminal units for persons in charge. *Each terminal unit is allocated a unique function in advance.* The server sends the document with verification data appended to the first terminal unit in a predetermined route (a route for circulation). Each terminal unit sends the document directly to a next terminal unit in the predetermined route and **applies its unique function to the verification data in turn when receiving the document.** The last terminal unit in the predetermined route sends the document with verification data back to the server. Upon receipt of the electronic document that has been circulated through the terminal units for persons in charge, the server examines the function-applied value appended to the document to determine

whether the document has been circulated correctly through the persons in charge, or via the correct route. However, Komura et al. fails to teach a server which is responsible for any processing relating to identification and encryption/decryption of the document.

Summary of Akama (U.S. Application Publication No. 2002/0062440)

Akama is directed to a proxy facility for facilitating the exchange of encryption keys between a home terminal and an electronic marketplace server. The proxy facility initiates a communication between the home terminal and the electronic marketplace to establish a common key between the two computing devices. The devices can subsequently communicate by using the common key that was exchanged between the home server and the electronic market server. Akama fails to teach or suggest a document processing server that processes electronic documents between senders and recipients in which the senders and recipients do not exchange keys.

Summary of An et al. (U.S. Patent No. 6,715,073)

An et al. discloses a system and method for *managing* the issuance, renewal, and revocation of *digital certificates* for Web browsers and servers using vault technology. Generally, the vault technology provides a secure environment in a web server using a vault controller for running a secure Web-based registration process and enabling secure application. The controller provides security from other processes running on the same server and secure areas, or personal storage vaults to which only the owner has a key. System operators, administrators, certificate authorities, registration authorities, and others cannot get to stored information or secure processes in such personal vaults. The system in An et al. includes registration and certification authorities, and a Web server (vault controller) maintaining personal storage vaults in the controller for users. Each personal vault runs programs on the controller under a unique UNIX user ID. This particular UNIX user ID is linked to a user with a specific vault access certificate. The content of the vault is encrypted and contains an encryption key pair and a signing key pair, both of which are password protected. Data storage provided by the

controller is owned by the same user ID assigned to the vault. A registration authority running as a software application in the controller processes requests to issue, renew and revoke **digital certificates issued by a certification authority using two pairs of public-private keys.**

Examiner's Interview Summary

Applicant thanks the Examiner for taking time on August 17, 2007, to participate in a telephone interview. The interview was conducted in light of the Office Action rejecting Claims 1-3, 12-15, 17, 20-28, 32-36, and 38-65. Participating in the August 17, 2007, interview were the Examiner and applicant's representative, Sunah Lee. The discussion in the interview was directed to the distinction between the independent claims and the prior art, particularly the citations of Claims 1, 19, and 37.

Rejection of Claims 1, 3, 5-7, 10, 12-19, 24-26, 30-37, 42-45, and 47-49 Under 35 U.S.C. § 103(a)

As indicated above, Claims 1, 3, 5-7, 9, 10, 12-19, 24-26, 30-37, 41-45, and 47-49 were rejected under 35 U.S.C. § 103(a) as being obvious over Komura et al. in view of Akama. As described in more detail below, applicant respectfully disagrees.

Claim 1

As amended, Claim 1 recites:

> 1. A method for a document processing server to process communications between a sender and at least one recipient and to verify an identity of the sender and the at least one recipient for establishing a secured communication channel, the method comprising:
>
> at the document processing server:
>
> obtaining a request from the sender to transmit an electronic document to at least one recipient;
>
> obtaining an electronic document corresponding to the request from the sender, wherein the electronic document is encrypted with an encryption key corresponding solely to the sender and the document processing server processing the electronic document wherein processing the electronic document includes encrypting the electronic document with an encryption key corresponding solely to at least one recipient and the document processing server;

verifying the identity of the designated at least one recipient and the identity of the sender;

upon verification, establishing a secured communication channel with the at least one recipient;

transmitting the processed electronic document to the designated at least one recipient;

wherein the sender and the designated at least one recipient do not verify the identity of each other; and

wherein the sender and the designated at least one recipient do not share encryption keys.

Claim 1 recites a method for a document processing server to process communications between a sender and at least one recipient and to verify an identity of the sender and the at least one recipient for establishing a secured communication channel to transmit a document. In particular, Claim 1 includes the limitations of "obtaining an electronic document corresponding to the request from the sender, wherein the electronic document is encrypted with an encryption key corresponding solely to the sender and the document processing server" and "processing the electronic document wherein processing the electronic document includes encrypting the electronic document with an encryption key corresponding solely to at least one recipient and the document processing server," both of which are done "at the document processing server." Additionally, Claim 1 recites "verifying the identity of the designated at least one recipient and the identity of the sender" at the document processing server so that "the sender and the designated at least one recipient do not verify the identity of each other," or "the sender and the designated at least one recipient do not exchange encryption keys."

Applicant agrees with the Office Action, Komura et al. does not teach or suggest verifying the identity of the recipient and verifying the identity of the sender in order to transmit a document from the sender to the recipient. In direct contrast, as taught in Komura, the sender and the recipient verify the identity of each other upon an exchange of an electronic document. In Komura, each terminal sends the document directly to a next terminal in the predetermined route and appends verification data, such as a digital signature, before sending the documents to the next terminal. Upon receipt of the document, "a signature verification unit" of a recipient

terminal verifies the verification data appended to documents received from a sender terminal and, after verification, the recipient terminal applies its unique function to verification data.

For example, Col. 6, lines 44-50, of Komura et al. discloses:

> In procedure P3, the terminal 12 sends the document, the ID code, the function-applied value, and **the digital signature** 1 from its interface 41 to the interface 51 of the terminal 13. Upon receipt of the information via the interface 51, **the signature verification unit 52 verifies the digital signature appended by the person in charge 1.** If the digital signature is verified as that appended by the person in charge 1, the function application unit 53 applies the function 2 stored in the function storage unit 55 to the received function-applied value. The **signature creating unit 54 then appends the digital signature 2 to the document**, the ID code, and the function-applied value "function 2 (function 1 (value)). (Emphasis added.)

As described in the above-cited passage, a sender terminal sends "the document, the ID code, the function-applied value, and **the digital signature**" to a recipient terminal. Subsequently, "the signature verification unit" in the recipient terminal verifies "the digital signature appended by the person in charge" of the sender terminal unit. For the reasons set forth above, Komura et al. fails to teach "verifying the identity of the designated at least one recipient and the identity of the sender" at the document processing server so that "the sender and the designated at least one recipient do not verify the identity of each other."

The Office Action states that Komura et al. inherently teaches "the sender and the designated at least one recipient do not share encryption keys," as recited in Claim 1. Specifically, the Office Action argues that Komura et al. teaches the utilization of the public encryption key system. One of ordinary skill in the art would understand that a public key in the public key encryption system serves the purpose of encrypting and decrypting a particular secret key that is **exchanged** between a sender and a recipient. Regardless of whether Komura, or another other reference, teaches the utilization of a proxy to facilitate that transmission of encryption keys, all of the cited references teaches a sharing of an encryption key (i.e., an encrypted secret key which is use to encrypt data) between a sender and a recipient. Applicant respectfully submits that Akama has been cited for the specific purpose of teaching a proxy

server for facilitating the sharing of encryption keys between a recipient and a sender. This is contrary to the above mentioned limitation recited in Claim 1. In fact, applicant respectfully submits that Komura, and Akama for the same reason, would not function in the manner intended if a sender and recipient did not share encryption keys as specifically recited with regard to Claim 1.

Under 35 U.S.C. § 103(a), a *prima facie* case of obviousness is established only if the cited references, alone or in combination, teach each of the limitations of the recited claims. *In re Bell*, 991 F.2d 781 (Fed. Cir. 1993). For the reasons set forth above, applicant respectfully submits that Komura et al. and Ana, alone or combination, fails to expressly or inherently teach, disclose, or suggest each and every element of Claim 1. Specifically, as explained above, Komura et al. fails to disclose or suggest "verifying the identity of the designated at least one recipient and the identity of the sender" at the document processing server so that "the sender and the designated at least one recipient do not verify the identity of each other," or "the sender and the designated at least one recipient do not exchange encryption keys." Accordingly, applicant respectfully submits that amended Claim 1 is allowable and requests that the rejection be withdrawn.

Claims 3, 5-7, 10, 12-18, and 47

Claims 3, 5-7, 10, 12-18, and 47 depend from Claim 1. For the reasons discussed above with regard to Claim 1, applicant respectfully submits that the cited reference fails to teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the rejection of Claims 3, 5-7, 10, 12-18, and 47 under 35 U.S.C. § 103(a).

Claim 19

As amended, Claim 19 recites:

> 19.   A system for processing communications, the system comprising:
> a sender computing device configured to transmit a request to process an electronic document;

at least one recipient computing device corresponding to an identifiable communication channel; and

a document processing server, the document processing server configured to verify the identities of the sender computing device and the at least one recipient computing device and to establish secure communications with the sender computing device and the at least one recipient computing device;

wherein the document processing server processes an electronic document and transmits the processed electronic document between the sender computing device and the recipient computing device without the sender computing device and the at least one recipient computing device sharing encryption keys and wherein the document processing server processes the electronic documents with an encryption key corresponding solely to the document processing server and the recipient computing device ; and

wherein the sender computing device and the at least one recipient computing device do not verify the identity of each other.

Applicant respectfully submits that Komura et al. and Akama, alone or in combination, fail to teach or suggest each and every limitation recited in Claim 19. For example, the cited references fail to teach "a document processing server, the document processing server configured to verify the identities of the sender computing device and the at least one recipient computing device and to establish secure communications with the sender computing device and the at least one recipient computing device" so that "the sender and the at least one recipient do not verify the identity of each other," as recited in Claim 19. As stated above, Komura et al. discloses a server computing device (server) that is patentably distinguishable over a document processing server as recited in Claim 19. The server in Komura et al. does not verify each of the designated recipients or transmit the document to each of the designated recipients. Instead, each terminal unit in Komura et al. verifies the verification data upon receipt of the document, applies its unique function, appends a digital signature, and sends the document to a next terminal unit. Similarly, Akama teaches a proxy server for facilitating the sharing of encryption keys between a recipient and a sender, For those reasons stated above, the cited references fail to teach each and every limitation recited in Claim 19. Applicant respectfully requests withdrawal of the rejection of Claim 19 under 35 U.S.C. § 103(a).

Claims 24-26, 30-36, and 48

Claims 24-26, 30-36, and 48 depend from Claim 19. As discussed above, the cited references fail to teach or suggest each of the limitations recited in Claim 19. For the above mentioned reasons with regard to Claim 19, applicant respectfully submits that the cited reference fails to teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the rejection of Claims 24-26, 30-36, and 48 under 35 U.S.C. § 103(a).

Independent Claim 37

For similar reasoning with respect to Claims 1 and 19, applicant submits that Komura et al. or Akama, alone or in combination, do not teach "a document processing component configured to verify the identity of the one of the plurality of recipient computing devices and the sender computing device and to process document requests from the sender computing device and append to the document at least an electronic signature corresponding to the sender" and "the document processing server processes the electronic documents with an encryption key corresponding solely to the document processing server and the recipient computing device" as recited in Claim 37. As described above, the server disclosed in Komura, in view of Akama, does not "verify the identity of the one of the plurality of recipient computing devices and the sender computing device" but each computing device has to verify each other for a secure communication. Accordingly, the cited references fail to teach each and every limitation recited in Claim 37. Applicant respectfully requests withdrawal of the rejection of Claim 37 under 35 U.S.C. § 103(a).

Claims 41-45 and 49

Claims 41-45 and 49 depend from Claim 37. As discussed above, the cited references fail to teach or suggest each of the limitations recited in Claim 37. For the reasons discussed above with regard to Claim 37, applicant respectfully submits that the cited reference fails to

teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the rejection of Claims 41-45 and 49 under 35 U.S.C. § 103(a).

Rejection of Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 Under 35 U.S.C. § 103(a)

The Office Action rejected Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 under 35 U.S.C. § 103(a) as being unpatentable over Komura et al. in view Akama further in view of An et al. The Office Action submits that cited references suggest each and every element of these claims and that it would be obvious to combine the teachings of the references. Applicant respectfully disagrees.
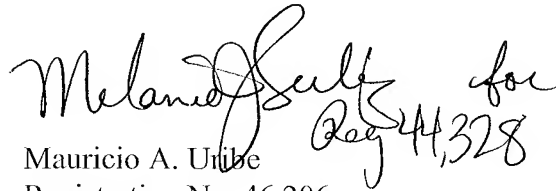
As described above, a primary reference, Komura, fails to teach, or suggest all the limitations of Claims 1, 19, and 37. As also mentioned above, Akama not make up the defects of Komura. Still further, applicant submits that An et al. does not make up the defects of Komura et al. and/or Akama, alone or combination. An et al. merely teaches a system and method for managing the issuance, renewal, and revocation of digital certificates for Web browsers and servers using vault technology. However, the method disclosed in An et al. has nothing to do with "verifying the identity of the designated at least one recipient and the identity of the sender" at the document processing server so that "the sender and the designated at least one recipient do not verify the identity of each other," or "the sender and the designated at least one recipient do not exchange encryption keys," as recited in Claim 1. Similarly, the system disclosed in An et al. has nothing to do with "a document processing server" or "a document processing component" which is configured to verify the identities of a sender and recipients, as recited in Claims 19 and 37. As set forth above, the defects of Komura et al. and Akama cannot be cured by An et al. For these reasons, Komura et al. and An et al., alone or in combination, fail to disclose or suggest each limitation recited in Claims 1, 19, and 37. Claims 2, 4, 8, and 11 depend from Claim 1. Claims 20-23 and 27-29 depend from Claim 19. Claims 38-40 depend from Claim 37. Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 also include a myriad of recitations not disclosed, taught, or suggested by any of the cited and applied references, particularly when the recitations are

MSFT\18402AM4.doc
10/30/07 14:10 A10/P10

considered in combination with the recitations of claims from which these claims depends. Accordingly, applicant respectfully requests withdrawal of the rejection of Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 under 35 U.S.C. § 103(a) and allowance of the claims.

CONCLUSION

In view of the foregoing remarks, applicant submits that all pending claims are in patentable condition and respectfully requests an early notice to that effect. The Examiner is requested to contact applicant's attorney at the number provided below should any questions or issues remain.Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

Mauricio A. Uribe
Registration No. 46,206
Direct Dial No. 206.695.1728

MAU:tmm